

Basic Constraints Extension

References: X.509 sections: 12.1, 12.4.2.1, K.1
 RFC 2459 sections: 4.1.2.6, 4.2, 4.2.1.2, and 4.2.1.10
 FPKI Profile sections: 1.2.11, 3.2.2.1
 MISPC sections: 1.4, 2.1.1, and 3.1.3.3
 DII PKI Functional Specification sections: 3.2.2.3,
 3.2.4.1.1

Implementation under analysis:**Analysis Date:**

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
When the implementation issues a CA certificate is the basic constraint (BC) extension present, critical and its cA component set to TRUE?		
When the implementation issues a self-signed certificate is the basic constraint (BC) extension present, non-critical and its cA component set to TRUE?		
When the implementation issues a CA certificate, is the subject field populated with a non-empty distinguished name?		
When the implementation issues a CA certificate, is the subject key identifier extension present?		
CAs can request certificates from hierarchically superior CAs. Is an entity making such a certificate request identified as a CA through the basicConstraints extension?		
Does the application processing the certificate recognize the BC extension?		
In processing a received certificate, if the BC extension is present and flagged non-critical, and the cA component is TRUE, does the certificate user recognize it as a self-signed certificate?		
In processing a received certificate, if the BC extension is present,		

REQUIREMENT FROM STANDARDS	MET (Y/N/na)	NOTES
A received certificate has the BC extension present, flagged critical, the cA component is TRUE, and the pathLenConstraint value is 0. Does the certificate user recognize that the certificate subject can only issue EE certificates?		
A received certificate has the BC extension present, flagged critical, the cA component is TRUE, and the pathLenConstraint value is an integer greater than 0. Does the certificate user constrain the number of CA certificates that follow this certificate in the certification path to the value given?		
A received certificate has the BC extension present, flagged critical, the cA component is TRUE, and the pathLenConstraint field is absent. Does the certificate user recognize that there is no limit to the certification path length?		
In processing a received certificate, if the BC extension is not present, does the certificate user recognize it as an EE certificate?		
In processing a received certificate, if the BC extension is present and SEQUENCE is empty, does the certificate user recognize it as an EE certificate?		
In processing a received certificate, if the BC extension is present, flagged critical and the cA component is FALSE, does the certificate user recognize it as an EE certificate?		

Other information:

In processing a received certificate, if the certificate fails validation what does the implementation do?

None of processing cases is prohibited by the standards, so implementations should be capable of receiving and processing them. Issuing CA certificates is mandatory for implementations.

Recommendations for Standards Work:

RFC 2459 states that the BC extension should not appear in EE certificates. Early versions of the RFC (in I-D form) did not have this recommendation. The Federal and DOD specifications were based on the early I-Ds, and they have not been updated to reflect the published RFC. Recommend updating to reflect current IETF guidance.